Cassandra Crossing/ Tor è vivo? Tor è morto?

(71)— Circolano voci che danno per compromessa in modo definitivo una tecnologia di anonimizzazione che ha fin qui servito bene i suoi…

Cassandra Crossing/ Tor è vivo? Tor è morto?

Figure 1:

(71)— Circolano voci che danno per compromessa in modo definitivo una tecnologia di anonimizzazione che ha fin qui servito bene i suoi utenti. Ma i rumors non tengono conto della realtà. Tor c'è, oggi più che mai.

2 marzo 2007—No. Parafrasando Mark Twain, "*Le voci sulla compromissione di Tor sono state largamente esagerate*". E vediamo perché.

Tor è, con la sola eccezione di Freenet, il primo sistema per la privacy e l'anonimato ad essere distribuito ed utilizzato da utenti non specialisti e su larga scala. Pur essendo un sistema intrinsecamente complesso come Freenet, è al contrario semplice da usare ed integrabile con tutte le applicazioni di uso normale sulla Rete.

Al contrario di Freenet (che resta comunque un ottimo sistema per motivi che non ci interessano in questa sede) è a bassa latenza, veloce ed efficiente, pur rallentando (a volte parecchio) le applicazioni che lo usano.

Gli impazienti che dichiarano Tor "lento" non hanno evidentemente mai usato Mixmaster o Freenet; dovrebbero mettersi alla prova in questi ambienti per poter apprezzare il progresso che Tor rappresenta in termini di latenza e velocità. Privacy e fretta non sono mai andati d'accordo, specialmente in Rete.

Il risultato finale di queste caratteristiche positive, ed in particolare del fatto di dover gestire in maniera efficiente la banda che i router Tor devono condividere ed utilizzare, è quello di una notevole complessità del protocollo e del software.

Nessun sistema informatico è perfetto, e quelli per la privacy non fanno certo eccezione. La classe dei sistemi di rete a cui Tor, Mixmaster, Mixminion e Freenet appartengono, quella delle "Mix-net" teorizzata da Chaum nel 1981, possiede delle caratteristiche intrinseche che la rendono teoricamente suscettibile a certi tipi di attacchi. Tor è stato in pratica dimostrato suscettibile ad alcuni di questi, che esamineremo più in dettaglio:

- [Attacchi DoS contro i directory server: Tor necessita di alcuni (attualmente 5) server che distribuiscano le informazioni sui router attivi ai client. Questi server possono essere attaccati tramite DoS (Denial of Service—negazione del servizio) o tramite avvocati. Contro questo tipo di attacco l'unica difesa è aumentare il numero dei directory server e porli in diverse giurisdizioni.]
- [Attacchi di sovversione contro i directory server: l'attacco di cui si parla in questi giorni appartiene a tale categoria. Utilizzando alcuni router modificati, un attaccante può mandare informazioni errate ai directory server millantando una banda ed un'efficienza molto grandi, in questo modo "attraendo" il traffico dei client. Aumenta di conseguenza l'eventualità che un dato client utilizzi per realizzare il collegamento tre dei router compromessi, od almeno che ne usi due come ingresso e uscita. In questo modo l'anonimato della connessione (non necessariamente il suo contenuto) può essere violato.]
- [Attacchi di intercettazione dal router di uscita: il gestore di un router di uscita si trova nella posizione ideale per portare un attacco Man-in-the-middle contro le connessioni criptate (ed a maggior ragione contro quelle in chiaro) che lo utilizzano, falsificando lo scambio di certificati. Non si tratta di una debolezza di Tor, ma semplicemente del fatto che il router di uscita agisce come punto di scambio obbligato. Per rendere efficace questo attacco l'utente deve comunque accettare un certificato (visibilmente diverso) senza controllarlo. Qualunque sistema crittografico può essere violato se l'utente non controlla le credenziali che riceve e se non usa cura ed attenzione.]
- [Attacchi di compromissione degli hidden service: questo tipo di attacchi, di cui sono note due varianti, si basano sul fatto, piuttosto difficoltoso da rilevare con precisione, che una CPU più utilizzata si scalda o che un sistema molto caricato ha piccole variazioni di velocità del clock.]
- [Attacchi di marcatura del routing: questo tipo di attacchi cerca di riconoscere caratteristiche peculiari dei vari segmenti che compongono una connessione fatta attraverso Tor (o più in generale attraverso una Mixnet) sfruttandone caratteristiche particolari e/o creando ad arte connessioni riconoscibili.]
- [Attacchi di analisi temporale del traffico: questo è l'unico attacco a cui chi usa Tor è realmente sottoposto, e non deriva da un difetto ma da un pregio, una caratteristica di successo di Tor, quella di essere un sistema a bassa latenza. Tutti i sistemi a bassa latenza sono suscettibili ad attacchi portati da un attaccante di alto profilo in grado di monitorare una grossa parte del traffico scambiato. La meccanica dell'attacco è elementare. Se un client od un server ricevono o trasmettono per un periodo breve un traffico maggiore del solito, questo picco si "propaga" attraverso la rete Tor come un picco di traffico tra alcuni router particolari con temporizzazioni precise permettendo, almeno su base statistica, di compromettere parzialmente o totalmente l'anonimato dato da Tor (o da una qualsiasi altra Mixnet esistente o concepibile).]

Tutti questi attacchi sono ben documentati in alcuni lavori accademici, tutti rigorosamente in inglese e reperibili, talvolta con difficoltà, in vari posti in Rete. Per agevolare chi volesse approfondire il tema (attività vivamente consigliata) li ho raccolti in un unico archivio compresso,

scaricabile qui, che contiene anche la specifica originaria di Tor e la roadmap prevista per il 2007 per quanto riguarda ricerche, modifiche e nuovi sviluppi.

Chi avesse bisogno di documentazione in italiano puo' invece trovare alcuni documenti tradotti (ma purtroppo non le paper) qui.

Per concludere: Tor sta bene, è un mezzo robusto e ben progettato per ottenere livelli alti di privacy e di anonimato in ambiti precisi. Non è stato "craccato" nella sua concezione di base, e nessuno degli attacchi fino ad oggi noti potrebbe essere portato senza mezzi molto grandi o senza che almeno gli amministratori dei dirserver lo rilevassero.

L'attacco pubblicizzato la settimana scorsa lascerebbe tracce evidenti sui dirserver, e richiederebbe comunque mezzi non piccoli. Come altre tecnologie per la privacy, e come tutte le tecnologie, ha dei limiti precisi e non è una "pallottola d'argento" per tutti i problemi.

E' pero' l'applicazione più efficace e popolare, almeno come numero di utenti, e proprio per questo è insieme a Freenet l'unica ad aver trovato posto sui media tradizionali. Viene trattata da questi come altre notizie di carattere tecnologico, cioè spesso con un occhio speciale solo alla risonanza che può avere, e trascurando invece la precisione della notizia.

E' necessario inoltre sottolineare come il fatto di ricercare e trovare debolezze è l'unico modo per avere sistemi sempre più sicuri, e che gli scopritori di nuovi attacchi sono spesso gli stessi sviluppatori di Tor, od almeno lavorano a stretto contatto con loro.

Solo una politica di "Full Disclosure" porta un reale progresso verso la sicurezza e la privacy delle comunicazioni. A riprova di questo fatto la roadmap 2007 di Tor, inclusa nell'archivio di cui sopra e comunque reperibile sul sito, include evoluzioni volte a prevenire gli attacchi scoperti od anche solo ipotizzati.

Magari tutte le applicazioni per la privacy (ed anche tutte le altre) fossero sviluppate con questa cura progettuale ed accademica!Un parere finale personale: usate Tor con fiducia (ed accortezza, of course): la vostra privacy sarà incomparabilmente migliore.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 30, 2023.

Canonical link

Exported from Medium on August 27, 2025.